GDPR

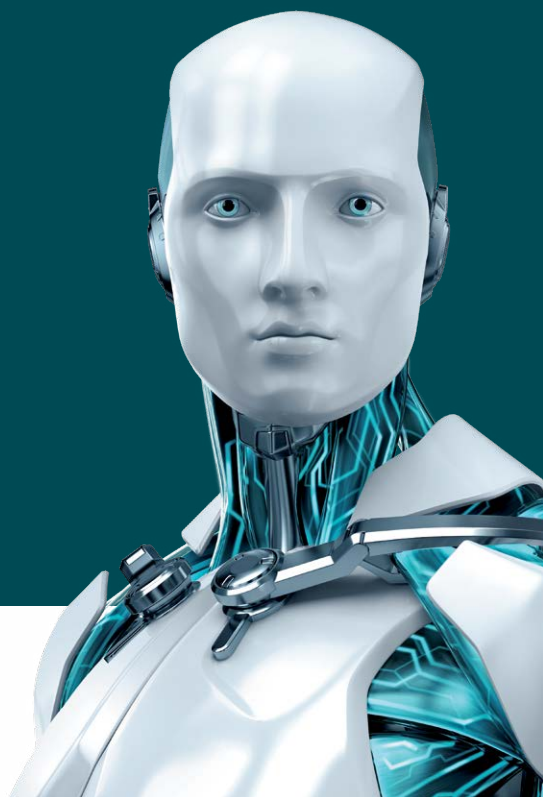
marec 2017

GDPR ŠPECIÁL

Praktický návod na prežitie pre

- **e-shopy**
- **agentúry vykonávajúce prieskumy trhu**
- **ostatné sektory – prehľadová tabuľka**

Viac informácií na tému GDPR
sifrovanie.eset.sk



ESET UŽÍVAJTE SI BEZPEČNEJŠIE TECHNOLÓGIE™

ALLEN & OVERY

Obsah

PRE E-SHOPY, MARKETINGOVÉ AGENTÚRY A ICH ZÁKAZNÍKOV

Nové nariadenie o ochrane osobných údajov[1] (**GDPR**), ktoré nahradí zákon č. 122/2013 Z.z. o ochrane osobných údajov, sa začne sa uplatňovať od 25. mája 2018. GDPR je obsiahly dokument, ktorý ovplyvní fungovanie mnohých spoločností. GDPR bude mať najväčší dopad na veľké spoločnosti, ktoré spracúvajú značné množstvo osobných údajov (respektíve pre spoločnosti, ktoré spracúvajú údaje, ktoré možno považovať za citlivé[2], napríklad údaje o zdravotnom stave). To však neznamená, že malé spoločnosti s menšími databázami sa GDPR vyhnú, respektíve že GDPR nebude obsahovať pre tieto spoločnosti žiadne povinnosti. Kým spoločnosti s veľkými databázami budú pravdepodobne musieť pozorne čítať každé ustanovenie GDPR, na spoločnosti s menšími databázami sa niektoré z ustanovení GDPR vzťahovať nebudú. To v každom prípade znamená, že práca na zabezpečovaní súladu s GDPR by nemala začať až v roku 2018, ale omnoho skôr.

Každá spoločnosť, ktorá spracúva osobné údaje, by teda mala vykonať interný audit a posúdiť, do akej miery sa jej GDPR dotýka, a aké zmeny bude musieť vykonať na to, aby jej fungovanie bolo od 25. mája 2018 v súlade s GDPR.

Zabezpečenie súladu s GDPR by sa nemalo riešiť len na nižších stupňoch v rámci hierarchie spoločnosti, respektíve len na právnom oddelení spoločnosti. Keďže GDPR pokuty za nerešpektovanie jej ustanovení posúva až do výšky **20 miliónov eur** alebo až do výšky **4% celosvetového ročného obratu** spoločnosti v predchádzajúcom finančnom roku, zabezpečenie súladu s GDPR by malo patriť medzi priority aj pre výkonné orgány spoločností (ako napríklad predstavenstvo alebo spoločníkov).

AKO SI PORADIŤ S GDPR

Ešte predtým, ako sa spoločnosť začne zamýšľať nad tým, ktoré ustanovenia GDPR bude musieť implementovať a na čo sa v rámci svojich činností zameria, je vhodné zamyslieť sa nad nasledovnými aspektmi:

1. **Určiť kompetentnú osobu pre otázky GDPR v rámci spoločnosti**. To znamená určiť, kto v rámci danej spoločnosti rozumie otázke ochrany osobných údajov a bude vedieť posúdiť dopad GDPR na konkrétnu spoločnosť. Touto osobou môže byť buď zodpovedná osoba (ak ju spoločnosť v minulosti mala) alebo aj právnik spoločnosti (v súčinnosti s technickými špecialistami). Ak taká osoba v rámci spoločnosti nie je, je vhodné vyhľadať experta externe.
2. **Data mapping**. Následne je potrebné definovať, aké osobné údaje spoločnosť spracúva. Povaha a rozsah dát budú určujúce pre množstvo povinností, ktoré bude musieť daná spoločnosť v rámci GDPR splniť.
3. **Prioritizácia**. Súlad s GDPR, najmä vo väčších spoločnostiach, nebude možné robiť naraz pre všetky databázy obsahujúce osobné údaje. Podľa množstva dát spracúvaných spoločnosťou alebo ich citlivosti bude treba určiť priority. Nakoľko GDPR je obsiahla legislatíva, bude

1 Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

2 **Citlivé osobné údaje** GDPR definuje ako tie, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, biometrických údajov na individuálnu identifikáciu fyzickej osoby, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby.

potrebné zvážiť riziká a určiť:

I. ktoré databázy sú v rámci spoločnosti najobjemnejšie,

II. ktoré databázy obsahujú citlivé osobné údaje,

III. prípadne iné „potenciálne slabé miesta" spoločnosti týkajúce sa osobných údajov (napríklad väčšia databáza s osobnými údajmi je outsourcovaná na spracúvanie tretej strane).

Súlad s GDPR by sa mal prioritne začať vykonávať práve v týchto oblastiach a následne sa presunúť k ostatným databázam.

4. **Vnútropodnikový „step-plán"**: Po tom, ako spoločnosť určí prioritné oblasti, ktoré berú do úvahy riziká, bude potrebné určiť zamestnancov, ktorí budú zodpovední za implementáciu jednotlivých krokov. Bude potrebné najmä:

   I. Určiť, či databáza neobsahuje viac údajov než je nevyhnutne potrebné,

   II. Definovať správny právny základ pre spracúvanie (napríklad súhlas, zmluva a podobne),

   III. Zrevidovať informáciu poskytnutú dotknutým osobám respektíve politiku ochrany súkromia (Privacy Policy),

   IV. Zrevidovať zmluvy so sprostredkovateľmi, ktorým boli outsourcované niektoré činnosti týkajúce sa osobných údajov,

   V. Zrevidovať bezpečnostné opatrenia (a ubezpečiť sa, či sú dostatočné),

   VI. Zrevidovať postup, ako spoločnosť nakladá so žiadosťami dotknutých osôb (napríklad žiadosť o výmaz osobných údajov alebo žiadosť o prenesenie osobných údajov) a posúdiť, či status quo je v súlade s postupmi a termínmi podľa GDPR,

   VII. Zrevidovať procesy pre oznamovanie porušení osobných údajov (aby spoločnosť bola schopná vykonať oznámenie v rámci určených termínov).

Táto štúdia obsahuje príkladný postup zabezpečenia súladu s GDPR pre dva typy spoločností:

1. Menšiu/stredne veľkú spoločnosť – zvolili sme e-shop; a
2. Väčšiu spoločnosť, ktorá je súčasťou nadnárodnej skupiny – zvolili sme spoločnosť vykonávajúcu prieskumy trhu pre iné spoločnosti (klientov).

1. PRÍKLAD 1: E-SHOP

PRE KTORÉ FIRMY JE TENTO PRÍKLAD VHODNÝ: Pre väčšinu firiem, ktoré prevádzkujú internetový obchod alebo poskytujú svoj tovar alebo služby prostredníctvom internetovej stránky

1.1 Aké dáta štandardne spracúva e-shop?

E-shop bude mať s najväčšou pravdepodobnosťou primárne nasledovné databázy obsahujúce osobné údaje:

1. Databáza zamestnancov (respektíve iných pracovníkov[3]). Táto databáza bude štandardne obsahovať identifikačné údaje zamestnancov, údaje o ich dochádzke, mzdových podmienkach, čerpaní dovolenky, prípadne o ich zamestnaneckých benefitoch.[4]
2. Dabatáza zákazníkov (môže zahŕňať databázu zákazníkov, ktorí si objednali tovar, respektíve databázu zákazníkov, ktorým sú po kúpe tovaru zasielané marketingové informácie spoločnosti). Táto databáza bude štandardne obsahovať údaje o zákazníkovi, aký tovar si objednal, adresu, kde mu bude zaslaný tovar, prípadne emailovú adresu, telefónne číslo, údaje o predchádzajúcich nákupoch, či údaje o preferenciách zákazníka.

Pri takýchto databázach bude musieť podľa GDPR e-shop splniť najmä nasledovné povinnosti.[5]

1.2 Informácia o spracúvaní osobných údajov

V prvom rade bude musieť spoločnosť **prepracovať Politiku ochrany súkromia** (Privacy Policy), ktorú má umiestnenú na svojej webovej stránke. Rozsah informácií, ktoré bola spoločnosť prevádzkujúca e-shop povinná poskytnúť podľa zákona č. 122/2013 Z.z. o ochrane osobných údajov je totiž odlišný od podmienok, ktoré stanovuje GDPR. Rovnako bude spoločnosť povinná poskytnúť novú informáciu o spracúvaní osobných údajov aj svojím zamestnancom.

Pri GDPR je rozsah informácií, ktoré treba zákazníkom (respektíve zamestnancom) poskytnúť, širší ako podľa zákona na ochranu osobných údajov (napríklad je potrebné uviesť dĺžku uchovávania údajov alebo informáciu o prípadnom profilovaní).

1.3 Sprostredkovateľská zmluva

Nakoľko stredne veľké (respektíve aj niektoré menšie) spoločnosti zvyknú často outsourcovať mzdovú agendu externým spoločnostiam, bude potrebné **prepracovať sprostredkovateľskú zmluvu**, ktorú má e-shop uzavretú s externou spoločnosťou, na ktorú tieto činnosti outsourcovala. Rovnako bude potrebné postupovať aj v prípade, ak zasielanie marketingových informácií (informácie o novinkách alebo špeciálnych akciách spoločnosti) tým zákazníkom, ktorí o to prejavili záujem, bolo outsourcované externej spoločnosti. Sprostredkovateľská zmluva podľa GDPR bude musieť obsahovať viac záruk ako podľa súčasného zákona o ochrane osobných údajov. E-shop by mal teda začať rokovania o revízii sprostredkovateľskej zmluvy čím skôr, aby nové zmluvy boli uzavreté do mája 2018.

3 Títo zamestnanci spravujú e-shop, vybavujú objednávky, odpovedajú na otázky (prípadne prevádzkujú menšiu kamennú predajňu) a pod.

4 Stredne veľké (a niektoré menšie) spoločnosti si často mzdovú agendu nespravujú sami, ale ju outsourcujú na správu externým spoločnostiam.

5 Výpočet povinností, ktoré bude musieť spoločnosť podľa GDPR splniť je iba demonštratívny.

1.4 Profilovanie[6]

Ak by e-shop pri svojej činnosti využíval profilovanie zákazníkov, ktoré sa bude robiť automatizovanou formou, musí sa v rámci GDPR zamerať aj na nové pravidlá pre profilovanie. O vytváranie profilov pôjde napríklad, ak cielený marketing alebo špeciálna ponuka, bude zaslaná len niektorým zákazníkom, podľa toho, či ich softvér zaradí do istého profilového koša (ktorého podmienky vytvorí e-shop[7]). Podľa toho, či zákazník spadne do istého profilového koša, mu môže spoločnosť ponúkať iné ponuky ako ostatným zákazníkom.

Takéto profilovanie, ak je založené len na automatizovanom spracúvaní[8], je možné len s **výslovným súhlasom** jednotlivca, ktorý má byť súčasťou profilovania. Takýto súhlas musí obsahovať dostatočné a jasné informácie o samotnom profilovaní a musí obsahovať možnosť nesúhlasiť s profilovaním. Profilovanie sa nesmie vykonávať s citlivými osobnými údajmi[9] (ibaže by bol daný výslovný súhlas jednotlivca) a pri spracúvaní osobných údajov týkajúcich sa detí.

1.5 Data protection by design and by default

So zreteľom na povahu, na rozsah a účel spracúvania ako aj na riziká, ktoré sú so spracúvaním spojené, e-shop bude musieť určiť primerané technické a organizačné opatrenia pre každú databázu obsahujúcu osobné údaje. Tieto opatrenia musia byť vybraté na základe najnovších poznatkov a technológií, avšak aj s prihliadnutím na ich cenu. Princípy ochrany súkromia musia byť komplexne posúdené pri koncipovaní každej kampane už od jej ranného štádia.

Privacy by design and by default bude v tomto konkrétnom prípade okrem technických požiadaviek ochrany dát zahŕňať najmä implementáciu **princípu minimalizácie údajov**. Minimalizácia údajov znamená, že e-shop bude musieť implementovať primerané technické a organizačné opatrenia, aby zabezpečil, že štandardne jeho systémy budú spracúvať len osobné údaje, ktoré sú nevyhnutne potrebné (a žiadne iné) pre každý konkrétny účel spracúvania. Rovnako musí byť zabezpečené, že sa údaje nebudú spracúvať neobmedzene, ale len na nevyhnutnú dobu. Osobné údaje nesmú byť štandardne prístupné neobmedzenému počtu zamestnancov, ale len zamestnancom, ktorí nevyhnutne potrebujú prístup k týmto osobným údajom.

1.6 Oznamovanie porušení ochrany osobných údajov[10]

V prípade, že e-shopu (alebo jeho komerčným partnerom) po máji 2018 dáta (respektíve ich časť) uniknú alebo sa stratia alebo nastane iné porušenie osobných údajov, nebude môcť e-shop takúto situáciu riešiť iba interne ako tomu bolo doteraz, ale bude musieť **informovať o takomto incidente Úrad na ochranu osobných údajov SR** (ďalej „**Úrad**"). Informácia o takomto incidente musí byť Úradu oznámená bez zbytočného odkladu, avšak nie dlhšie ako 72 hodín od momentu, keď sa spoločnosť o porušení dozvedela. Ak by táto lehota nemohla byť dodržaná, musí byť omeškanie oznámenia (teda dôvody prečo nebolo možné oznámiť do 72 hodín) zdôvodnené.

6 „**Profilovanie**" definuje GDPR ako akúkoľvek formu automatizovaného spracúvania osobných údajov, ktoré pozostáva z použitia týchto osobných údajov na vyhodnotenie určitých osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým analýzy alebo predvídania aspektov dotknutej fyzickej osoby súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním polohou alebo pohybom.

7 Napríklad podľa množstva nákupov, obvodu kde zákazník býva, správania sa zákazníka, preferencií a pod.

8 Bez možnosti ľudskej intervencie.

9 Napríklad ak e-shop bude robiť prieskum u svojich zákazníkov, ktorého súčasťou by boli otázky týkajúce sa zdravotného stavu.

10 „**Porušenie ochrany osobných údajov**" GDPR definuje ako porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene, neoprávnenému poskytnutiu osobných údajov, ktoré sa prenášajú, uchovávajú alebo inak spracúvajú, alebo neoprávnený prístup k nim.

Okrem oznámenia porušenia osobných údajov Úradu budú musieť byť v niektorých prípadoch informovaní o porušení aj jednotlivci (napríklad zákazníci), ktorých dáta sú incidentom dotknuté. Avšak pokým oznámenie Úradu bude potrebné vykonať takmer pri každom porušení, oznámenie jednotlivcom bude potrebné vykonať len v tých najzávažnejších prípadoch. E-shop by si teda mal vypracovať interný plán pre oznamovanie a následné riešenie incidentov, ktoré zahŕňajú porušenie ochrany osobných údajov.

GDPR obsahuje širokú škálu ďalších povinností. Tie však budú relevantné pre menší (stredne veľký) e-shop iba marginálne alebo nebudú relevantné vôbec.[11]

ESET Endpoint Encryption

Zašifrovaním osobných údajov uložených vo vašich systémoch sa vyhnete pokute pri prípadnom úniku dát. Osobám, ktorých údaje unikli, zároveň nebudete musieť tento incident nahlasovať.

Šifrovacie riešenie spoločnosti ESET je výkonné, možno ho jednoducho nasadiť, a dokáže bezpečne zašifrovať pevné disky, vymeniteľné médiá, súbory a e-maily.

Získajte viac informácií na www.eset.sk/sifrovanie

2. PRÍKLAD 2: SPOLOČNOSŤ VYKONÁVAJÚCA PRIESKUM TRHU

PRE KTORÉ FIRMY JE TENTO PRÍKLAD VHODNÝ: marketingové agentúry, prieskumné agentúry, zákazníci takýchto spoločností, agentúry, ktoré spracúvajú dáta iných klientov (outsourcing), cloud provideri

2.1 Aké dáta štandardne spracúva spoločnosť vykonávajúcu prieskum trhu pre iné spoločnosti?

Táto spoločnosť bude mať s najväčšou pravdepodobnosťou primárne nasledovné databázy obsahujúce osobné údaje:

1. Databázu svojich vlastných zamestnancov,
2. Databázu respondentov (t.j. osôb, ktoré poskytli tejto spoločnosti súhlas, že ňou môžu byť kontaktovaní v prípade, že prieskum trhu bude zahŕňať parametre, ktoré spĺňajú),
3. Prípadne databázu osôb, ktorú agentúra vykonávajúca prieskum trhu dostane od svojich klientov, ktorí zadávajú parametre žiadaného prieskumu[12].

Pri takýchto databázach bude musieť agentúra vykonávajúca prieskum trhu splniť najmä nasledovné povinnosti podľa GDPR.[13]

11 Práva ako právo byť zabudnutý, právo na prenos údajov zrejme nebudú pre menší/stredne veľký e-shop príliš relevantné. Rovnako podľa GDPR nebude potrebné nominovať zodpovednú osobu. Ak e-shop vyššie popísaný bude pôsobiť iba na Slovensku, tak jeho dozorným orgánom bude Úrad na ochranu osobných údajov SR. Ak by mala spoločnosť zriadené pobočky aj v iných krajinách je potrebné určiť, kde sa nachádza miesto centrálnej správy (teda miesto, kde sa prijímajú rozhodnutia). To bude do značnej miery determinované umiestnením hlavnej prevádzky spoločnosti. Prenosy do tretích krajín pravdepodobne tiež nebudú relevantné, ibaže by e-shop napríklad používal na úschovu dát o svojich klientoch resp. zamestnancoch dátové centrum (napr. cloud), ktoré by bolo umiestnené mimo krajín EÚ/Európskeho hospodárskeho priestoru.

12 Tieto osoby však musia poskytnúť súhlas s tým, aby ich klient mohol ďalej sprístupniť agentúre vykonávajúcej prieskum trhu.

13 Výpočet povinností, ktoré bude musieť spoločnosť podľa GDPR splniť je iba demonštratívny.

2.2 Informácia o spracovaní osobných údajov

Ako pri prvom prípade, spoločnosť bude musieť prepracovať informáciu o spracovaní osobných údajov, ktorú poskytla respondentom, ktorých využíva na zodpovedanie otázok relevantných pre prieskum. Rozsah informácií, ktoré bola spoločnosť povinná poskytnúť podľa zákona o ochrane osobných údajov je totiž odlišný od podmienok, ktoré stanovuje GDPR. Ako bolo uvedené vyššie, pri GDPR je rozsah informácií, ktoré treba jednotlivcom poskytnúť, širší. Rovnako bude spoločnosť povinná poskytnúť novú (rozšírenú) informáciu o spracúvaní osobných údajov aj svojím zamestnancom.

2.3 Prepracovanie súhlasov

S najväčšou pravdepodobnosťou bude potrebné zrevidovať súhlasy respondentov byť kontaktovaný agentúrou v prípade, že ich odpovede môžu byť pre prieskum potrebné. Súčasne poskytnuté súhlasy (podľa zákona o ochrane osobných údajov) budú môcť byť považované za platné len do tej miery, pokiaľ budú reflektovať nové požiadavky GDPR. Keďže však zákon o ochrane osobných údajov obsahoval menej podmienok na platný súhlas ako GDPR, je dôvodný predpoklad, že agentúra vykonávajúca prieskum trhu si bude musieť vyžiadať od respondentov nové súhlasy. Čo sa týka súhlasov poskytnutých zamestnancami, počet takýchto súhlasov bude musieť byť zrejme zredukovaný vzhľadom na problematickosť poskytnutia súhlasu v rámci zamestnaneckého pomeru[14]. Ponechané by mali byť iba súhlasy, kde má zamestnanec reálne (bez problémov a bez akejkoľvek ujmy) možnosť súhlas odmietnuť. Odporúča sa akékoľvek súhlasy poskytnuté v rámci pracovnej zmluvy presunúť na separátny dokument.

2.4 Úloha agentúry vykonávajúcej prieskum trhu ako sprostredkovateľa

V prípade, ak agentúra vykonávajúca prieskum trhu pracuje s údajmi, ktoré patria klientovi (a nie s „vlastnými" respondentmi), napríklad prieskum trhu sa vykonáva iba so zákazníkmi klienta (napríklad s dátami držiteľov vernostných kariet klienta)[15], agentúra bude voči takýmto dátam v úlohe sprostredkovateľa. To znamená, že **dáta nepatria agentúre, ale klientovi**, a agentúra s týmito dátami pracuje len v rámci inštrukcií, ktoré jej poskytne klient, a po skončení projektu dáta klientovi vráti alebo ich vymaže. Podľa zákona o ochrane osobných údajov väčšinu zodpovedností mali prevádzkovatelia (v tomto prípade to bude klient agentúry, pre ktorého sa vykonáva prieskum), nakoľko sa jednalo o „ich" údaje (resp. údaje „ich" zákazníkov). Prevádzkovatelia boli zodpovední za súlad so zákonom aj v prípadoch, ak niektoré činnosti outsourcovali na externé spoločnosti (sprostredkovateľov).

GDPR túto situáciu mení a **sprostredkovatelia majú po prvý krát na základe GDPR priame povinnosti ochrany osobných údajov**, a to napriek tomu, že nespracúvajú osobné údaje vo vlastnom mene, ale pre klienta. Sú to okrem iných (i) povinnosť viesť zoznamy spracovateľských operácií, a to pre každého klienta (prevádzkovateľa) zvlášť, a (ii) v prípade porušenia ochrany osobných údajov musia sprostredkovatelia informovať prevádzkovateľa.

Rovnako GDPR reguluje, čo má obsahovať **sprostredkovateľská zmluva** (zmluva medzi prevádzkovateľom a sprostredkovateľom). Obsah tejto zmluvy bude odlišný od požiadaviek zákona o ochrane osobných údajov. Je teda dôvodné (a oprávnené), ak klient ešte pred májom 2018 osloví

14 Z dôvodu nerovnakého postavenia medzi zamestnancom (prevádzkovateľom) a zamestnancom, kde zamestnanec (z obavy, že môže prísť o prácu) reálne nemôže nesúhlasiť a teda vzniká obava, že súhlas nebude mať základný atribút pre svoju platnosť (nakoľko nie je slobodne daný).

15 Alebo držiteľmi bonusových programov klienta.

agentúru so žiadosťou o prepracovanie (doplnenie) uzatvorenej sprostredkovateľskej zmluvy, ktorá bola uzavretá podľa zákona o ochrane osobných údajov. Nad rámec štandardných požiadaviek[16] spracovateľskej zmluvy bude potrebné do každej takejto zmluvy zahrnúť mnoho ďalších dojednaní ohľadne záruk ochrany osobných údajov, a to napríklad aj právo vykonať audit.[17]

2.5 Data protection by design and by default

Tak ako pri prvom príklade, so zreteľom na povahu, rozsah a účel spracúvania ako aj na riziká, ktoré sú so spracúvaním spojené, agentúra vykonávajúca prieskum trhu bude musieť určiť **primerané technické a organizačné opatrenia** pre každú databázu obsahujúcu osobné údaje. Tieto opatrenia musia byť vybraté na základe najnovších poznatkov a technológií, avšak aj s prihliadnutím na ich cenu. Princípy ochrany súkromia musia byť komplexne posúdené pri koncipovaní každej kampane, už od jej ranného štádia.

Rovnako ako je uvedené vyššie, privacy by design and by default bude okrem technickým požiadaviek ochrany dát zahŕňať najmä implementáciu **princípu minimalizácie údajov** a garanciu, že sa údaje nebudú spracúvať neobmedzene, ale len na nevyhnutnú dobu. Osobné údaje nesmú byť štandardne prístupné neobmedzenému počtu zamestnancov, ale len zamestnancom, ktorí nevyhnutne potrebujú prístup k týmto osobným údajom. Pri mnohých prieskumoch bude vhodné zvážiť aj **pseudonymizáciu** údajov[18] a vykonávať prieskumy s takto upravenými údajmi.

Agentúra môže využiť nový certifikačný mechanizmus, ktorý zavádza GDPR[19], ako napríklad schválené pečate a značky na preukázanie súladu s požiadavkami „privacy by design and by default".

2.6 Oznamovanie porušení osobných údajov

Je logické, že ak povinnosť oznamovať porušenia ochrany osobných údajov mal aj menší alebo stredne veľký e-shop, táto povinnosť neminie ani väčšiu spoločnosť pracujúcu s oveľa objemnejšími databázami.

V prípade, že spoločnosti po máji 2018 dáta (respektíve ich časť) uniknú alebo sa stratia alebo nastane iné porušenie osobných údajov, nebude môcť firma takúto situáciu riešiť iba interne ako tomu bolo doteraz, ale bude musieť **informovať o takomto incidente úrad**. Informácia o takomto incidente musí byť Úradu oznámená bez zbytočného odkladu, avšak nie dlhšie ako 72 hodín od momentu, keď sa spoločnosť o porušení dozvedela. Ak by táto lehota nemohla byť dodržaná, musí byť omeškanie oznámenia (teda dôvody prečo nebolo možné oznámiť do 72 hodín) zdôvodnené.

Okrem oznámenia porušenia osobných údajov Úradu budú musieť byť v niektorých prípadoch informovaní o porušení aj jednotlivci (napríklad zákazníci), ktorých dáta sú incidentom dotknuté.

16 Napríklad informácia o predmete a dobe spracúvania, účele spracúvania, type osobných údajov, kategórie dotknutých osôb a práv a povinností prevádzkovateľa.

17 Napríklad doplnenie ustanovení, (i) že sprostredkovateľ implementoval primerané bezpečnostné opatrenia na ochranu osobných údajov (napríklad pseudonymizáciu, šifrovanie, pravidelné skúšanie a hodnotenie účinnosti technických a organizačných opatrení či schopnosť včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu), (ii) detaily ohľadne subdodávok, a to najmä v tom zmysle, že ak sprostredkovateľ zapojí ďalšieho sprostredkovateľa, „pôvodný" sprostredkovateľ zostáva voči prevádzkovateľovi plne zodpovedný za plnenie povinností tohto ďalšieho sprostredkovateľa, (iii) záväzok že po ukončení poskytovania služieb sprostredkovateľ všetky osobné údaje prevádzkovateľa vymaže alebo vráti prevádzkovateľovi a vymaže existujúce kópie, (iv) záväzok sprostredkovateľa, že poskytne prevádzkovateľovi všetky informácie potrebné na preukázanie splnenia povinností podľa GDPR a umožní mu vykonať audit.

18 „**Pseudonymizácia**" je spracúvanie osobných údajov takým spôsobom, aby osobné údaje už nebolo možné priradiť ku konkrétnej dotknutej osobe bez použitia dodatočných informácií, pokiaľ sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia s cieľom zabezpečiť, aby osobné údaje neboli priradené identifikovanej alebo identifikovateľnej fyzickej osobe.

19 Certifikačné mechanizmy na účely preukázania súladu s GDPR.

Avšak pokým oznámenie Úradu bude potrebné vykonať takmer pri každom porušení, oznámenie jednotlivcom bude potrebné vykonať len v tých najzávažnejších prípadoch. Spoločnosti by si teda mal vypracovať interný plán pre oznamovanie a následné riešenie incidentov, ktoré zahŕňajú porušenie ochrany osobných údajov.

2.7 Posúdenie vplyvu na ochranu osobných údajov (Privacy Impact Assesment)

Nie je úplne vylúčené, že niektoré prieskumy budú obsahovať otázky, ktoré budú zahŕňať aspekty týkajúce sa zdravotného stavu alebo náboženského či politického vierovyznania. To budú údaje, ktoré budú patriť medzi takzvané „citlivé" osobné údaje[20]. Nakoľko prieskumy môžu zahŕňať spracúvanie takýchto dát vo veľkom rozsahu, v týchto prípadoch bude agentúra vykonávajúca prieskum trhu povinná ešte pred začatím spracúvania posúdiť vplyv takéhoto spracúvania na práva fyzických osôb (vypracovať takzvaný Privacy Impact Assessment). Rovnako budú citlivé údaje (napríklad údaje o zdravotnom stave) súčasťou databázy, ktorá bude obsahovať zamestnanecké dáta. Ak aj takáto databáza bude môcť byť považovaná za rozsiahlu, táto povinnosť sa bude (separátne) vzťahovať aj na túto databázu.

Tento dokument bude zahŕňať najmä:

1. opis plánovaných spracovateľských operácií a účely spracúvania,
2. posúdenie nutnosti a primeranosti vo vzťahu k účelu,
3. posúdenie rizík pre práva respondentov a
4. opatrenia na riešenie týchto rizík, vrátane bezpečnostných opatrení.

2.8 Prenosy osobných údajov do tretích krajín

Ak agentúra vykonávajúca prieskumy bude patriť do medzinárodnej skupiny, je možné, že dáta, ktoré, bude spracúvať, budú uložené na centrálnom serveri spoločnosti. To bude platiť najmä pre zamestnanecké dáta, ktorých uchovávanie bude pravdepodobne na spoločnom serveri pre celú skupinu. Tieto servery sa môžu nachádzať aj mimo krajín EÚ, resp. krajín Európskeho hospodárskeho priestoru (EHP)[21], napríklad v USA alebo v Ázii. V tom prípade takáto spoločnosť bude musieť prijať záruky pre prenos týchto zamestnaneckých dát do tretej krajiny. Do úvahy prichádza najmä uzavretie vnútro-skupinových štandardných zmluvných doložiek pre medzinárodný prenos alebo prijatie vnútropodnikových záväzných pravidiel[22], ktoré podpíšu všetky spoločnosti v rámci skupiny, ukladajúce dáta na centrálny server. Rovnaký režim sa uplatní aj v prípade, ak agentúra dáta na prieskum uchováva mimo centrálneho servera, napríklad v

20 Pozri poznámku pod čiarou č. 2.

21 Rovnaký režim ako pre krajiny EÚ (EHP) sa uplatní pre niektoré ďalšie krajiny, o ktorých bolo Európskou komisiou rozhodnuté, že ich úroveň ochrany osobných údajov je dostatočná (napríklad Izrael, Kanada, Monako, Argentína, Švajčiarsko, USA – spoločnosti, ktoré sa prihlásili k „Privacy Shield"). Na tieto krajiny sa teda hľadí ako na krajiny, ktorých právny systém dostatočne chráni súkromie dotknutých osôb, a teda dáta môžu byť prenesené.

22 Binding Corporate Rules (BCRs). BCRs však musia prejsť schvaľovacím procesom dozornými orgánmi v EÚ predtým ako bude možné ich použiť.

cloudovom riešení, ktoré je umiestnené mimo územia EÚ/EHP[23]. V takomto prípade bude potrebné ešte predtým, ako do takéhoto úložiska agentúra umiestni svoje dáta, prijať vhodné záruky pre prenos (pravdepodobne najideálnejšími budú štandardné zmluvné doložky medzi agentúrou (ako vývozcom údajov) a cloud providerom ako príjemcom údajov[24]).

Rovnako sa tento systém uplatní, ak klient vyžaduje, aby agentúra pracovala s dátami, ktoré patria klientovi (a ktoré agentúre pre účely vypracovania prieskumu dočasne poskytne), ak sú tieto dáta umiestnené mimo územia EÚ/EHP[25]. V tomto prípade je potrebné podotknúť, že dáta sa považujú za prenesené aj vtedy, ak ich agentúra na svoj server fyzicky od klienta neobdrží, ale iba dostane prístup na klientov server umiestnený mimo územia EÚ/EHP[26].

2.9 „One- stop- shop" (jednotné kontaktné miesto)

Princíp „one-stop-shop" sa použije najmä pri nadnárodných spoločnostiach, ktoré pôsobia vo viacerých štátoch. Tento princíp znamená, že pre takúto korporáciu sa v EÚ určí **vedúci dozorný orgán** a **dotknuté dozorné orgány**. Nejedná sa teda o úplnú centralizáciu dozoru takejto spoločnosti do rúk jedného dozorného orgánu s tým, že by ostatné dozorné orgány v ostatných členských štátoch EÚ úplne stratili nad touto korporáciou právomoci.

Spoločnosť si bude musieť určiť, v ktorej krajine bude vedúci dozorný orgán. **Vedúci dozorný orgán** (lead supervisory authority) bude riešiť zásadné otázky tejto korporácie a bude mať koordinačnú úlohu (napríklad pri vyšetrovaní, ktoré zahŕňa viacero jurisdikcií). **Dotknuté dozorné orgány** (supervisory authorities concerned) budú riešiť zvyšné otázky.[27]

Určenie, ktorý orgán je v rámci nadnárodnej korporácie pôsobiacej vo viac ako v jednom štáte v EÚ vedúcim dozorným orgánom, vôbec nie je podľa GDPR jednoduché. GDPR obsahuje komplexný a relatívne zložitý právnický matrix určenia tohto orgánu, založený na posúdení, kde má spoločnosť **miesto centrálnej správy v EÚ** (teda miesto, kde sa prijímajú rozhodnutia[28]). Často ňou bude materská spoločnosť resp. operačné ústredie skupiny.[29]

23 Alebo mimo územia, o ktorom bolo Európskou komisiou rozhodnuté, že jej úroveň ochrany osobných údajov je dostatočná (pozri poznámku pod čiarou č. 21).

24 Agentúra ako vývozca bude v pozícii prevádzkovateľa a cloud provider ako príjemca bude v pozícii sprostredkovateľa.

25 Alebo v krajine, o ktorej bolo Európskou komisiou rozhodnuté, že jej úroveň ochrany osobných údajov je dostatočná.

26 Klient ako vývozca bude v pozícii prevádzkovateľa a agentúra vykonávajúca prieskum trhu ako príjemca bude v pozícii sprostredkovateľa.

27 Napríklad ak bola sťažnosť podaná na dotknutom dozornom orgáne, vyšetrí ju tento dozorný orgán, na ktorom bola sťažnosť podaná, resp. ak sa spracúvanie týka len vybraného jedného štátu (napríklad prieskum sa týka len zákazníkov v jednej určitej krajine EÚ), rovnako sa ňou bude zaoberať tento orgán.

28 Prítomnosť technických prostriedkov (napríklad serverov) nie je relevantným kritériom pre určenie hlavnej prevádzkarne.

29 Aj keď spoločnosť si svoj vedúci dozorný orgán volí sama, táto determinácia nesmie byť svojvoľná podľa toho, v ktorom štáte by chcela dozorný orgán, ale musí takúto voľbu náležite preukázať, a to podľa kritérií stanovených pre hlavnú prevádzkareň.

3. VPLYV GDPR (VYBRANÉ ASPEKTY) NA OSTATNÉ SEKTORY

Sektor	Oznamovanie porušenia osobných údajov	Nominácia zodpovednej osoby	Prepracovanie súhlasov	Nové povinnosti pre sprostred-kovateľov	Privacy by design and by default	Medzinárodné prenosy dát
Letectvo, obrana	√√	√	√	√	√√	?
Automobily, náhradné diely	√√	x	√	√	√√	√
Bankovníctvo, finančné služby a poisťovníctvo	√√	√	√√	√√	√√	√√
Charitatívne organizácie a neziskový sektor	√√	x	√	x	√√	?
Farmaceutický priemysel, chemický priemysel, zdravotnícke služby	√√	√√	√√	√√	√√	√√
Služby	√√	x	√√	√√	√√	√
Stavebníctvo	√√	x	√	√	√√	√
Vzdelávanie	√√	x	√√	√	√√	√
Energetika	√√	√	√√	√	√√	√
Doprava	√√	√	√	√	√√	√
Potravinársky priemysel, FMCG[30], alkohol, tabak	√√	x	√√	√	√√	√√
Lesníctvo a papierový priemysel	√√	x	√	√	√√	?
Verejný sektor	√√	√√	√	x	√√	x
Televízia, médiá, telekomunikácie	√√	x	√√	√√	√√	√√
Softvér	√√	√	√√	√√	√√	?
Poľnohospodárstvo	√√	x	√	x	√√	?
Marketing, PR	√√	√	√√	√√	√√	√

Vysvetlivky

√√	Daný segment GDPR určite ovplyvní
√	Daný segment GDPR pravdepodobne ovplyvní
x	Daný segment GDPR pravdepodobne neovplyvní
xx	Daný segment GDPR určite neovplyvní
?	Nie je možné určiť, či daný segment GDPR ovplyvní (bude to záležať od konkrétnych okolností)

30 Fast moving consumer goods.

Právne závery obsiahnuté v tejto publikácii boli spracované advokátskou kanceláriou Allen & Overy Bratislava, s.r.o.

Zuzana Hečko
Advokátka
Allen & Overy Bratislava, s.r.o.
Zuzana.Hecko@allenovery.com

ESET, spol. s r.o
Obchodné oddelenie
Tel.: +421 (2) 322 44 250
obchod@eset.sk

GDPR READY

SIFROVANIE.ESET.SK

ESET

ENDPOINT ENCRYPTION

Vaša najlepšia voľba pre šifrovanie dát

Jednoducho použiteľná ochrana dát v súlade s GDPR, vhodná pre firmu akejkoľvek veľkosti.

BEZPEČNOSTNÍ IT EXPERTI
NA VAŠEJ STRANE